

COMPLEXITY OF LP IN TERMS OF THE FACE LATTICE

ALEKSANDR MAKSIMENKO

ABSTRACT. Let X be a finite set in \mathbb{Z}^d . We consider the problem of optimizing linear function $f(x) = c^T x$ on X , where $c \in \mathbb{Z}^d$ is an input vector. We call it a *problem* X . A problem X is related with linear program $\max_{x \in P} f(x)$, where polytope P is a convex hull of X . The key parameters for evaluating the complexity of a problem X are the dimension d , the cardinality $|X|$, and the encoding size $S(X) = \log_2 \left(\max_{x \in X} \|x\|_\infty \right)$. We show that if the (time and space) complexity of some algorithm A for solving a problem X is defined *only* in terms of combinatorial structure of P and the size $S(X)$, then for every d and n there exists polynomially (in d , $\log n$, and S) solvable problem Y with $\dim Y = d$, $|Y| = n$, such that the algorithm A requires exponential time or space for solving Y .

1. INTRODUCTION

In many cases a combinatorial optimization problem can be stated in the following form.

GIVEN a finite set of feasible solutions $X \subset \mathbb{Z}^d$, and a linear function $f(x) = c^T x$, $c \in \mathbb{Z}^d$, $x \in X$.

FIND the maximum (minimum) value of $f(x)$.

We will call it a *problem* X , assuming an arbitrary choice of the input vector $c \in \mathbb{Z}^d$. For example, in the travelling salesman problem the set X , $X \subset \{0, 1\}^E$ is the set of characteristic vectors of hamiltonian circuits in a graph $G = (V, E)$.

A problem X is related with linear program (LP)

$$\max_{x \in P} c^T x, \quad \text{where } P = \text{conv } X.$$

This is the main reason of interest to such geometric statement of a combinatorial optimization problem.

It is clear that the complexity of a problem X may depend on the encoding size¹

$$(1) \quad S(X, c) = \log_2 \left(\max_{x \in X \cup \{c\}} \|x\|_\infty \right).$$

But $S(X, c)$ does not reflect the structural complexity of X .

So, it is natural to consider some combinatorial characteristics of $P = \text{conv } X$ as characteristics of complexity of a problem X . The simplest examples are the dimension of P , the number of its vertices, and the number of its facets. Nontrivial

Supported by the project No. 477 of P.G. Demidov Yaroslavl State University within State Assignment for Research.

¹This is the natural requirement for the modern digital devices.

examples are the diameter of the graph (1-skeleton) of P , the clique number of the graph, and the rectangle covering number of the vertex-facet (non)incidence matrix.

The diameter of the graph of P was considered as the lower bound of complexity of a problem² $X = \text{ext } P$ in the class of simplex-type algorithms. The weakness of this bound is illustrated by the following well known example. For any (arbitrary complicated) polytope P one can consider a pyramid Q with P as a base. It is obvious that the problem $Y = \text{ext } Q$ is not simpler than the problem $X = \text{ext } P$, but the graph diameter of a pyramid is not greater than 2.

In 1980's, V. A. Bondarenko introduced the concept of so-called direct type algorithms [2, 3]. The main idea is that the clique number of the graph of $\text{conv } X$ is the lower bound on the complexity of the appropriate problem X in this class of algorithms. We discuss this theory and its limitations in the section 2. In particular, we show that there is no an algorithm whose complexity for solving a problem X is expressed only in the clique number of the graph of $\text{conv } X$ and in the encoding size $S(X, c)$.

Polytope Q is called an *extension* (or extended formulation) of a polytope P if there is a linear projection π with $\pi(Q) = P$. In this context, the number of facets of a polytope is frequently called a *size* of a polytope. It is well known that the size of an extension Q may be significantly less than the size of its projection P . On the other hand the problem $\max_{x \in P} c^T x$ is easily reduced to the problem $\max_{y \in Q} b^T y$.

Thus in some cases it is usefull to express a polytope P via its extension. The minimum size of an extension of a polytope P is called *extension complexity* of P .

In the end of 1980's, M. Yannakakis in his seminal paper [17] on extended formulations noticed that the extension complexity is bounded from below by the rectangle covering number of the vertex-facet (non)incidence matrix. Several breakthrough results was obtained in this direction over the past three years (see [6], [7], [16]). All of them suggest that there may exist an algorithm whose complexity for solving a problem X is equal to big O (or some polynomial) of the rectangle covering number. In the section 3 we enumerate this facts and show that there is no such algorithm.

Our main result is presented in the section 4. Let the function f takes each problem X to \mathbb{N} . We assume that f is defined only in terms of the face lattice of $\text{conv } X$ and the encoding size $S(X, c)$, and f is monotone in $S(X, c)$ and the face lattice (by embedding). (I.e. the function f is a monotone combinatorial characteristic of complexity of X .) Then there are an exponentially solvable problem Y and a polynomially solvable problem Z such that $f(Y) \leq f(Z)$.

2. DIRECT TYPE ALGORITHMS

2.1. Introduction to the theory. The information in this subsection is not crucial for the rest of the paper, but it seems that there is no description of the theory of direct type algorithms in English. So we have to say "a couple of words" about this interesting theory [2, 3].

² X is the set of extreme points of P

First of all we should say that direct type algorithms are *linear search algorithms* (LSAs). When dealing with LSAs, one takes into account only time necessary for branchings of the form “if $f(c) > 0$ then goto α , else goto β ” [13]. Here $c \in \mathbb{R}^d$ is the input vector of a problem X and $f(c) = a^T c + b$ is an affine function, where $a \in \mathbb{R}^d$, $b \in \mathbb{R}$. It is convenient to imagine the structure of an LSA as a *linear decision tree* (LDT) with tests “ $f(c) > 0$ ” in internal nodes. Every terminal node (leaf) of such tree has some label $x \in X$. (One label $x \in X$ can be assigned to more than one leaf.)

The *complexity* $C_{LSA}(X)$ of a problem X is the minimum depth of an LDT for X . Clearly, $C_{LSA}(X) \geq \log |X|$ (provided that for every $x \in X$ there exists an input c s.t. x is the optimal solution). In [14] (see also [15]) the upper bound $O(d^3 \log |X|)$ have been found for $C_{LSA}(X)$. But such LSA can occupy an exponential space. So, it would be good to add some natural restrictions to LSA model.

In 1980th, V.A. Bondarenko introduced the concept of so-called *direct type algorithms* [2]. This concept is based on the notion of partition of \mathbb{R}^d into cones. For every $x \in X$ we consider its cone

$$K(x) = \{c \in \mathbb{R}^d \mid c^T x \geq c^T y, \forall y \in X\}.$$

The set of all such cones for given X is called a *partition of \mathbb{R}^d into cones w.r.t. X* . It is clear, that $K(x)$ is not empty iff x lies on the boundary of the convex hull $\text{conv } X$. In particular, if $X \subseteq \{0, 1\}^d$ then every $x \in X$ is a vertex of $\text{conv } X$ and, hence, every $K(x)$ has interior points. Traditionally, the convex hull $\text{conv } X$ is called *the polytope of a problem X* . Typically, the set X coincides with the set of vertices of the polytope $\text{conv } X$. Here and below we assume the latter condition is fulfilled. I.e., for every $x \in X$ there exists $c \in K(x)$ such that $c^T x > c^T y$ for any $y \in X$, $y \neq x$.

Two cones $K(x)$ and $K(y)$ are called *adjacent* if

$$\exists c \in K(x) \cap K(y) : c^T x = c^T y > c^T z \quad \forall z \in X, z \neq x, z \neq y.$$

It is obvious that $K(x)$ and $K(y)$ are adjacent iff the vertices x and y of the polytope $\text{conv } X$ are adjacent (i.e., these vertices form a 1-face of the polytope). The subset $Y \subseteq X$ is called a *clique in X* if every pair $\{x, y\} \subseteq Y$ is adjacent.

Let T is a linear decision tree for a problem X and f is some internal node of T . Let $L(f)$ is the set of leaves of T that are descendants of f . We denote by X_f , $X_f \subseteq X$, the set of labels of leaves $L(f)$. The set $L(f)$ is divided into two parts $L^+(f)$ and $L^-(f)$ by two arcs outgoing from f . Let X_f^+ and X_f^- denote all the labels of leaves $L^+(f)$ and $L^-(f)$, respectively.

Definition 1 ([2]). A linear decision tree for solving a problem X is called *direct type tree* if for any internal node f and for any clique $Y \subseteq X$ the following inequality holds:

$$|X_f \cap Y| - 1 \leq \max\{|X_f^+ \cap Y|, |X_f^- \cap Y|\}.$$

The *complexity* $C_{DTT}(X)$ of X is the minimum depth of a direct type tree for a problem X .

Let $\omega(X)$ is the size of the maximum clique in X . I.e. $\omega(X)$ is the clique number of the 1-skeleton of $\text{conv } X$. It is not difficult to see that

$$C_{DTT}(X) \geq \omega(X) - 1.$$

It is known [2, 3], that sorting algorithms, greedy algorithms for the minimum spanning tree, Dijkstra's algorithm for the shortest path in a graph, Held-Karp algorithm and branch-and-bound algorithms for the travelling salesman problem, and some other combinatorial algorithms are direct type algorithms. On the other hand, clique numbers $\omega(X)$ are superpolynomial for such NP-hard problems as the travelling salesman, the knapsack, the 3-satisfiability, the 3-assignment, the maximum cut, the set covering, the set packing and many others [2, 11, 12]. Whereas $\omega(X)$ are polynomial for polynomially solvable problems: the sorting, the minimum spanning tree, the short path in a graph, the min-cut problem [2, 4].

Nonetheless, there are examples of polynomially solvable problems X with exponential $\omega(X)$ [2]. A generalization of one such example is considered in the following subsection.

It is also natural to ask the following question.

Question 1 (V. Kaibel). Is there some (NP-)hard problems with small $\omega(X)$?

2.2. Examples. The first example is related with the famous cyclic polytopes. (More detailed information on cyclic polytopes is presented in [8].) Let us consider a monotone function

$$(2) \quad g : \mathbb{N} \rightarrow \mathbb{N}, \quad g(i) < g(i+1) \quad \forall i \in \mathbb{N},$$

and the set

$$(3) \quad C(d, N, g) = \{(t_i, t_i^2, \dots, t_i^d) \in \mathbb{N}^d \mid t_i = g(i), i \in [N]\},$$

where $d, N \in \mathbb{N}$. The convex hull of $C(d, N, g)$ is a cyclic polytope. It is well known that d -dimensional cyclic polytope is a simplicial $\lfloor d/2 \rfloor$ -neighborly polytope and it has the maximum number of faces among all convex polytopes with the same number N of vertices [8]. In particular, the clique number $\omega(C(d, N, g)) = N$ for $d \geq 4$.

Theorem 2. *A problem $C(d, N, g)$ is solvable polynomially in d and $\log N$ whenever the function g is polynomially countable and the encoding size of an input vector c is polynomial in d and $\log N$. In particular, if $g(i) = i$, $i \in \mathbb{N}$ and $\|c\|_\infty = O(N)$, then the solving of a problem $C(d, N, g)$ requires $O(d^4 \log^2 N)$ time and $O(d \log N)$ space.*

Proof. We have to maximize function $c^T x = c_1 x_1 + c_2 x_2 + \dots + c_d x_d$ for $x \in C(d, N, g)$. That is we have to maximize the polynomial

$$f(t) = c_1 t + c_2 t^2 + \dots + c_d t^d, \quad \text{where } t = g(i), i \in [N].$$

The algorithm of finding the maximum will consist of $d - 1$ steps.

In the first step we divide the set $[N]$ into (two or one) segments where the derivative $f^{(d-1)}(t) = (d-1)! c_{d-1} + d! c_d t$ has constant sign.

In the second step we consider the derivative

$$f^{(d-2)}(t) = (d-2)! c_{d-2} + \frac{(d-1)!}{1!} c_{d-1} t + \frac{d!}{2!} c_d t^2.$$

It is monotone in every segment found in the previous step. Hence it is not difficult to divide every such segment into segments with constant sign of $f^{(d-2)}(t)$. It can

be done by dichotomic procedure and requires no more than $2 \log_2 N$ evaluations of $f^{(d-2)}(t)$.

In the following steps, by analogy we eventually partition the set $[N]$ into at most d segments with constant sign of $f'(t)$. Thus, it remains to find the value of $f(t)$ at the ends of these segments and choose the maximum.

To conclude the proof it remains to note that the calculation of $f'(t)$ requires $O(d)$ arithmetic operations with $(d \log g(N))$ -bit numbers. In particular, it takes $O(d^2 \log N)$ time for the case $g(i) = i$. \square

As a consequence, for every $k \in \mathbb{N}$ the problem $C(2k, 2^k, g)$ with $g(i) = i$ is solvable polynomially in k , but the clique number $\omega(C(2k, 2^k, g)) = 2^k$ is exponential. Moreover, $\text{conv } C(2k, 2^k, g)$ is k -neighborly. Hence, any its k vertices form a (simplicial) face.

It turns out that there are also examples of the opposite nature. More precisely, there are problems with $\omega(X) = 2$ and arbitrary complexity.

Theorem 3. *For any simplex $\Delta_d \subset \mathbb{R}^d$ there is an extension $Q \subset \mathbb{R}^{d+1}$ with $\omega(Q) = 2$.*

Proof. We use the fact that any two d -dimensional simplices are affinely equivalent to each other. So, we consider only the “simplest” one:

$$\Delta_{d-1} = \{x \in \mathbb{R}_+^d \mid x \in H\},$$

which is the intersection of a nonnegative orthant \mathbb{R}_+^d and a hyperplane

$$H = \{x = (x_1, \dots, x_d) \in \mathbb{R}^d \mid x_1 + \dots + x_d = 1\}.$$

We will construct an extension $Q \subset \mathbb{R}^d$ such that the projection of Q into the hyperplane H coincides with Δ_{d-1} . Therefore, Q is contained in the cylinder

$$Y = \left\{ x = (x_1, \dots, x_d) \in \mathbb{R}^d \mid (n-1)x_i + 1 \geq \sum_{j \neq i} x_j, \ i \in [d] \right\}.$$

Besides, let Q be symmetric with respect to H . So, we construct only half of Q that lies in $H^+ = \{x \in \mathbb{R}^d \mid x_1 + \dots + x_d \geq 1\}$. This half of Q we denote by Q^+ . Let Q^+ be the intersection of the cylinder Y , halfspace H^+ , and the unit cube $C_d = \{x \in \mathbb{R}_+^d \mid x \leq \mathbf{1}\}$. It is not difficult to see that the combinatorial structure of Q^+ is the combinatorial structure of the “cube without one vertex” $H^+ \cap C_d$. All vertices of Q^+ can be divided into d groups according to the number of coordinates equal to 1. The first group consists of one vertex $(1, 1, \dots, 1)$. Every vertex in the second group has one coordinate $\frac{d-2}{d-1}$ and $d-1$ ones. Every vertex in the third group has two coordinates $\frac{d-3}{d-2}$ and $d-2$ ones. The last group consists of d basis vectors.

We remark that every triangle in the graph of the polytope Q^+ is contained in H or has one edge in H . Thus, when we glue Q^+ and Q^- all triangles will disappear. Hence $\omega(Q) = 2$. \square

It is obvious that the linear optimization on the simplex Δ_d (in the general case) requires at least d^2 operations. The same is true for the optimization on its extension Q . Thus, in this example the dimension of the problem characterizes

the complexity much more accurately, than the clique number. Moreover, the theorem says that there is no an algorithm whose complexity for solving a problem X is expressed only in the clique number $\omega(X)$ and encoding size of X .

3. RECTANGLE COVERING NUMBERS

3.1. Background. Let $V = \{v_1, \dots, v_n\}$ be the set of vertices of a polytope P and $F = \{F_1, \dots, F_k\}$ be the set of its facets. The vertex-facet nonincidence matrix $A = (a_{ij}) \in \{0, 1\}^{n \times k}$ of P is defined as follows:

$$a_{ij} = \begin{cases} 0, & \text{if } v_i \in F_j, \\ 1, & \text{otherwise.} \end{cases}$$

Let $I \subseteq [n]$, $J \subseteq [k]$. The set $I \times J$ is called *1-rectangle* in A if $a_{ij} = 1$ for all $i \in I$ and $j \in J$. A *rectangle covering* of A is the set of 1-rectangles whose union is equal to union of 1-entries in A . The *rectangle covering number* of A is the smallest cardinality of a rectangle covering of A . By following [7] we denote by $\text{rc}(P)$ the rectangle covering number of the vertex-facet nonincidence matrix of P .

It is known, that the rectangle covering number is the lower bound on an extension complexity of P [17] (see [7] for the current knowledge on this topic). In particular, if some problem X (more precisely, its convex hull $\text{conv } X$) has a compact extended formulation, then $\text{rc}(\text{conv } X)$ is polynomial. At the present time, there are known a lot of polynomially solvable problems with compact extended formulations. Among them are sorting problems, spanning trees, matchings, cuts, approximation case of the knapsack problem and many others [5]. Special mention should be the perfect matching polytope $P_M(n)$. It has a polynomial rectangle covering number $\text{rc}(P_M(n)) = O(n^4)$ [7], but exponential extension complexity $\text{xc}(P_M(n)) = 2^{\Omega(n)}$ [16]. On the other hand, the boolean quadratic polytope (correlation polytope) BQP_n has exponential rectangle covering $\text{rc}(\text{BQP}_n) = 2^{\Omega(n)}$ [6] (see also [10] for the best current bound). Consequence of this result are super-polynomial lower bounds on rectangle covering numbers for many other NP-hard problems involving travelling salesman problem, knapsack problem, satisfiability problems, 3-assignment problem, set covering and set packing problems, and many others [6, 11, 12]. These facts let one to conjecture that the rectangle covering number is a complexity of some algorithm (or class of algorithms) for solving a problem X . It turns out that this is not true. We show that there are NP-hard problems with polynomial rc .

Our construction is based on the fact that $\text{rc}(P)$ of a simplicial polytope P is equal to $O(d^2 \log n)$ [7], where $d = \dim P$ is the dimension and $n = |\text{ext } P|$ is the number of vertices of P . The main idea is to make a slight perturbation of vertices of 0/1-polytope associated with NP-hard problem.

3.2. Cyclic Perturbation. For every $x \in \{0, 1\}^d$ we define its number

$$n(x) = \sum_{i=1}^d 2^{i-1} x_i, \quad 0 \leq n(x) \leq 2^d - 1.$$

Let us consider a map $\varepsilon : \{0, 1\}^d \rightarrow \mathbb{N}^d$ for transforming $x \in \{0, 1\}^d$ to $\varepsilon \in \mathbb{N}^d$:

$$\begin{aligned}\varepsilon_1 &= n(x), \\ \varepsilon_2 &= (n(x))^2, \\ &\dots \\ \varepsilon_d &= (n(x))^d.\end{aligned}$$

Let

$$K = 2^{d^3}$$

be “very big” constant. Note that for any $x \in \{0, 1\}^d$, the $\|\varepsilon(x)\|$ is “very small” with respect to K :

$$\frac{\|\varepsilon(x)\|}{K} \leq \frac{\|\varepsilon(x)\|_1}{K} \leq \frac{(2^d - 1) + (2^d - 1)^2 + \dots + (2^d - 1)^d}{K} \leq \frac{2^{d^2}}{2^{d^3}} = 2^{-d^2(d-1)}.$$

Let $X \subseteq \{0, 1\}^d$. The set

$$Y = \text{CP}(X) = \{y \in \mathbb{Z}^d \mid y = Kx + \varepsilon(x), x \in X\}$$

is called *cyclic perturbation* of X . It is clear that after such perturbation the encoding size of X increases in $\log_2 K = d^3$ times. Furthermore, $Y = \text{ext conv } Y$ since the value $\|\varepsilon(x)\|$ of perturbation is “very small”.

Lemma 4. *The convex hull of the cyclic perturbation of $X \subseteq \{0, 1\}^d$ is a simplicial polytope.*

Proof. It is sufficient to prove that any $d + 1$ points³ in the cyclic perturbation

$$Y = \text{CP}(X)$$

are affinely independent.

For every $(d + 1)$ -point set $\{y^1, y^2, \dots, y^{d+1}\} \subseteq Y$ we must check that

$$(4) \quad \det \begin{pmatrix} 1 & y_1^1 & y_2^1 & \dots & y_d^1 \\ 1 & y_1^2 & y_2^2 & \dots & y_d^2 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & y_1^{d+1} & y_2^{d+1} & \dots & y_d^{d+1} \end{pmatrix} \neq 0.$$

Since $y^i = Kx^i + \varepsilon(x^i)$ for some $x^i \in X$, $i \in [d + 1]$, we may decompose the matrix (4) into the sum of two matrices

$$A = \begin{pmatrix} 0 & Kx_1^1 & Kx_2^1 & \dots & Kx_d^1 \\ 0 & Kx_1^2 & Kx_2^2 & \dots & Kx_d^2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & Kx_1^{d+1} & Kx_2^{d+1} & \dots & Kx_d^{d+1} \end{pmatrix} \in \{0, K\}^{(d+1) \times (d+1)}$$

³We consider only interesting cases when $|\text{CP}(X)| \geq d + 1$. The other cases can be proved by analogy.

and

$$B = \begin{pmatrix} 1 & n(x^1) & (n(x^1))^2 & \dots & (n(x^1))^d \\ 1 & n(x^2) & (n(x^2))^2 & \dots & (n(x^2))^d \\ \dots & \dots & \dots & \dots & \dots \\ 1 & n(x^{d+1}) & (n(x^{d+1}))^2 & \dots & (n(x^{d+1}))^d \end{pmatrix}.$$

For every set $S \subseteq [d+1]$ we define $(d+1) \times (d+1)$ -matrix D^S :

$$D_{ij}^S = \begin{cases} A_{ij}, & \text{if } i \in S, \\ B_{ij}, & \text{if } i \notin S. \end{cases}$$

In particular, $D^{[d+1]} = A$, $D^\emptyset = B$. As is known, the determinant of the sum of two $n \times n$ -matrices can be written as the sum of determinants of 2^n matrices:

$$(5) \quad \det(A+B) = \sum_{S \subseteq [d+1]} \det D^S.$$

For every nonempty set S the matrix D^S has at least one row from A . Therefore, $\det D^S$ is a multiple of K . On the other hand, $\det D^\emptyset = \det B$ is the Vandermonde determinant:

$$\det B = \prod_{1 \leq j < k \leq d+1} (n(x^k) - n(x^j)) > 0.$$

Moreover,

$$\det B = \prod_{1 \leq j < k \leq d+1} (n(x^k) - n(x^j)) \leq (2^d - 1)^{d(d+1)/2} < K.$$

Hence, the sum (5) is not equal to 0. \square

Since $\text{rc}(P) = O(d^2 \log |\text{ext } P|)$ for any simplicial polytope $P \in \mathbb{R}^d$ [7], we immediately get

Corollary 5. *The rectangle covering number $\text{rc}(\text{conv } CP(X)) = O(d^2 \log |X|) = O(d^3)$ for any $X \subseteq \{0, 1\}^d$.*

Example 6. Let us consider the cyclic perturbation of vertices of the boolean quadratic polytope⁴

$$\text{BQP}_n = \left\{ x = (x_{ij}) \in \{0, 1\}^{n(n+1)/2} \mid x_{ij} = x_{ii}x_{jj}, 1 \leq i < j \leq n \right\}.$$

Obviously, the encoding size (in any reasonable sense) of BQP_n is polynomial in n . Hence, the same is true for its cyclic perturbation $\text{CBQP}_n = \text{CP}(\text{BQP}_n)$. Moreover, due to corollary 5, the rectangle covering number $\text{rc}(\text{conv } \text{CBQP}_n) = O(n^3(n+1)^2)$ is polynomial.

Now we show that the optimization problem CBQP_n is NP-hard. Let us consider the NP-hard problem of finding a clique number in an undirected graph $G = (V, E)$ with n vertices $V = [n]$. The input vector $c = c(G) \in \mathbb{Z}^{n(n+1)/2}$ we define as follows:

$$c_{ij} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } \{i, j\} \in E, \\ -2, & \text{if } \{i, j\} \notin E. \end{cases}$$

⁴Sometimes we use the same notation for the polytope and its vertices.

It is easy to see that $\max_{x \in \text{BQP}_n} c^T x$ is equal to the clique number of G . But for any $x \in \text{BQP}_n$ and $y = CP(x)$

$$|c^T x - c^T y/K| = |c^T \varepsilon(x)/K| \leq \frac{2}{2^{d^2(d-1)}} \leq \frac{1}{2^{17}},$$

where $d = n(n+1)/2$, $n \geq 2$. Hence the problem CBQP_n is not easy than the clique number problem.

4. THE MAIN RESULT

Let us denote by $\mathcal{F}(P)$ the set of all faces of a polytope P without improper faces \emptyset and P . The *face lattice* $\mathcal{L}(P)$ of a polytope P is the set $\mathcal{F}(P)$ (partially) ordered by inclusion. The face lattice $\mathcal{L}(P)$ of a polytope P is *embedded* into the face lattice $\mathcal{L}(Q)$ of a polytope Q if there is a map $h : \mathcal{F}(P) \rightarrow \mathcal{F}(Q)$ such that $F_1 \subseteq F_2$ iff $h(F_1) \subseteq h(F_2)$ for any two faces $F_1, F_2 \in \mathcal{F}(P)$. In such a case we will use the notation $\mathcal{L}(P) \preceq \mathcal{L}(Q)$.

In what follows we need the following example. Let $P \subset \mathbb{R}^d$ be a simplicial polytope with n vertices and let $C(2d, n) = \text{conv } C(2d, n, g)$ be a cyclic polytope with n vertices (see the equation (3)). Note that $C(2d, n)$ is d -neighborly (i.e. every d vertices form a (simplicial) face of $C(2d, n)$). Hence $\mathcal{L}(P) \preceq \mathcal{L}(C(2d, n))$. Moreover, for such embedding we get a several additional properties. The number of vertices and the number of facets of P do not exceed these numbers of $C(2d, n)$, the graph of P is a subgraph of the graph of $C(2d, n)$, and so on.

Let f be the map of face lattices to \mathbb{N} . We say that f is *monotone* if $f(\mathcal{L}(P)) \leq f(\mathcal{L}(C(2d, n)))$ for any simplicial d -polytope P with n vertices. It is natural to assume that combinatorial characteristics of complexity of a polytope must satisfy this property. Here are just a few examples of such functions: the dimension of a polytope, the number of its k -faces, the clique number of the graph, the maximum number of vertices of a k -neighborly face, the rectangle covering number. The monotonicity is not obvious only for the rectangle covering, but it is proved in [7, Corollary 2.13]. The diameter of the graph of a polytope is an example of a nonmonotone function.

In addition, when evaluating complexity of the problem $X \subset \mathbb{Z}^d$, we should take into account its size $S(X, c)$ (see equation (1)). If a (natural) function $f(X, c) = f(\mathcal{L}(\text{conv } X), S(X, c))$ is monotone in every argument, we call it a *monotone combinatorial characteristic of complexity* of a problem X . Below we restrict ourselves to the cases where the size of an input vector c does not make a significant contribution to $S(X, c)$ and we will write $f(X)$ instead of $f(X, c)$.

Theorem 7. *There exist an intractable problem X and a polynomially solvable problem Y such that $f(X) \leq f(Y)$ for any monotone combinatorial characteristic of complexity f .*

Proof. It is well known that almost all Boolean functions require exponential-sized circuits (see, for example, [1, Chapter 6]). Let $b : \{0, 1\}^d \rightarrow \{0, 1\}$ be such (intractable) function and

$$Z = \{z \in \{0, 1\}^d \mid b(z) = 1\}.$$

For each $x \in \{0, 1\}^d$ we define the input vector $c(x) \in \{-1, 1\}^d$ as follows:

$$c(x)_i = 2x_i - 1, \quad i \in [d].$$

It is easy to see that $\max_{z \in Z} (c(x))^T z$ is equal to the number of ones in x for $b(x) = 1$, otherwise it is less than the number of ones. Thus, the problem Z is intractable even for input $c \in \{-1, 1\}^d$. The same is true for the cyclic perturbation $X = \text{CP}(Z)$, since

$$|c^T z - c^T \text{CP}(z)/K| = |c^T \varepsilon(z)/K| \leq \frac{1}{2^{d^2(d-1)}} \leq \frac{1}{16}$$

for $c \in \{-1, 1\}^d$, $z \in Z$, and $d \geq 2$. Besides, the encoding size $S(X) = O(d^3)$ is polynomial and the polytope $\text{conv } X$ is simplicial.

To finish the proof we assume

$$Y = C(2d, |X|, g),$$

where $g : \mathbb{N} \rightarrow \mathbb{N}$ is a polynomially countable monotone function with $g(|X|) = 2^{S(X)}$. Thus, the problem Y is polynomially solvable by theorem 2. \square

Let us assume that the complexity of some algorithm A for solving a problem X is a monotone combinatorial characteristic of complexity of X . The theorem asserts that such an algorithm requires exponential (time or space) complexity for solving a problem $C(2d, |X|, g)$, but this problem is polynomially solvable by theorem 2. For example, the (polynomial of) rectangle covering number can not be a characteristic of complexity of such algorithm, since $\text{rc}(C(2d, |X|, g))$ is polynomial. But it may be considered as a lower bound. On the other hand, the clique number $\omega(C(2d, |X|, g)) = |X|$ is exponential in $\log |X|$. However, this characteristic violates more strict condition of monotonicity: the implication $\mathcal{L}(X) \preceq \mathcal{L}(Y) \Rightarrow f(X) \leq f(Y)$ should be true not only for $Y = C(2d, |X|, g)$. The appropriate example is provided by theorem 3.

5. CONCLUDING REMARKS

All the mentioned above combinatorial characteristics of complexity (with the exception of the diameter of the graph of a polytope) are monotone. We may ask the natural question: is the monotonicity a necessary condition? More precisely, are there an intractable problem X and a polynomially solvable problem Y with the same combinatorial structure and polynomially comparable encoding sizes $S(X)$ and $S(Y)$? This question is reduced to the following one. Is it true that one of the projections of a cyclic polytope $C(2d, |X|, g)$ is combinatorially isomorphic to a simplicial polytope X in theorem 7?

ACKNOWLEDGMENTS

The author is grateful to Volker Kaibel, Günter M. Ziegler, Matthias Walter, and Francisco Santos for helpful discussions.

REFERENCES

- [1] S. Arora and B. Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.
- [2] V.A. Bondarenko. *Graphs of polytopes and complexity in combinatorial optimization*. Yaroslavl': YarGU, 1995. (in Russian)
- [3] V.A. Bondarenko, A.N. Maksimenko. *Geometric constructions and complexity in combinatorial optimization*. Moscow: LKI, 2008. (in Russian)
- [4] Bondarenko, V.A., Nikolaev, A.V. Combinatorial and Geometric Properties of the Max-Cut and Min-Cut Problems. *Doklady Mathematics*, **88**(2), 516–517, 2013.
- [5] M. Conforti, G. Cornuéjols, and G. Zambelli. Extended formulations in combinatorial optimization. *A Quarterly Journal of Operations Research*, 8(1): 1–48, 2010.
- [6] S. Fiorini, S. Massar, S. Pokutta, H.R. Tiwary, R. de Wolf. Linear vs. semidefinite extended formulations: exponential separation and strong lower bounds. *In STOC*, 95–106, 2012.
- [7] S. Fiorini, V. Kaibel, K. Pashkovich, D.O. Theis. Combinatorial Bounds on Nonnegative Rank and Extended Formulations. *Discrete Math.*, 313(1): 67–83, 2013.
- [8] B. Grünbaum. *Convex Polytopes*. Second Edition prepared by V. Kaibel, V. Klee, and G.M. Ziegler, volume 221 of Graduate Texts in Mathematics, 2003.
- [9] V. Kaibel. Extended Formulations in Combinatorial Optimization. *Optima* 85, 2011.
- [10] V. Kaibel, S. Weltge. A Short Proof that the Extension Complexity of the Correlation Polytope Grows Exponentially. *arXiv:1307.3543*, 2013.
- [11] A.N. Maksimenko. The common face of some 0/1-polytopes with NP-complete nonadjacency relation. *Fundamentalnaya i prikladnaya matematika*, **18**(2), 105–118, 2013. (In Russian)
- [12] A.N. Maksimenko. A special place of Boolean quadratic polytopes among other combinatorial polytopes. *arXiv:1408.0948*, 2014.
- [13] F. Meyer auf der Heide. A polynomial linear search algorithm for the n -dimensional knapsack problem. *J. ACM*, **31**(3), 668–676, 1984.
- [14] M.Ju. Moshkov. On conditional tests. *DAN SSSR*, **265**(3), 550–552, 1982. (in Russian)
- [15] M.J. Moshkov. Time complexity of decision trees. *In Transactions on Rough Sets III*, Springer-Verlag, Berlin, Heidelberg, 244–459, 2005.
- [16] T. Rothvoss. The matching polytope has exponential extension complexity. *In STOC*, 263–272, 2014.
- [17] M. Yannakakis. Expressing combinatorial optimization problems by linear programs. *J. Comput. Syst. Sci.*, 43(3): 441–466, 1991.

LABORATORY OF DISCRETE AND COMPUTATIONAL GEOMETRY, P.G. DEMIDOV YAROSLAVL STATE UNIVERSITY, UL. SOVETSKAYA 14, YAROSLAVL 150000, RUSSIA
E-mail address: `maximenko.a.n@gmail.com`